Доклад на тему

Фильтрация спама

Автор: Авдадаев Джамал Геланиевич

Группа : НФИбд-02-23

Курс: Администрирование сетевых подсистем

Год: 2025

Введение

Электронная почта остаётся одним из основных инструментов коммуникации.Спам-сообщения составляют до 45–55% всего почтового трафика.Эффективная фильтрация спама снижает нагрузку на сеть и повышает безопасность пользователея

Список источников

Цель: Изучить современные методы фильтрации спама на уровне SMTP.

Задачи: Рассмотреть структуру и работу SMTP-протокола.

Изучить технологии SPF, Greylisting и SpamAssassin.

Показать практические подходы к настройке фильтрации.

Выводы

Протокол SMTP: краткий обзор

SMTP (Simple Mail Transfer Protocol) — стандартный протокол передачи электронной почты.

Основные команды: MAIL FROM, RCPT TO, DATA.

SMTP не предусматривает механизмов аутентификации отправителя — что и делает возможным спам..

Проблемы спама

Список источников

Подмена адреса отправителя (spoofing).

Массовая рассылка вредоносных писем.

Фишинг и рассылка ссылок на поддельные сайты.

Перегрузка серверов и ухудшение репутации домена.

SPF (Sender Policy Framework)

Проверяет, имеет ли IP-адрес право отправлять письма от имени домена.

Выводы

Использует DNS-записи типа TXT.

Помогает защититься от подделки адреса и фишинговых атак.

Пример SPF-записи:

v=spf1 ip4:192.0.2.0/24 include:_spf.google.com -all

Greylisting

Список источников

Сервер временно отклоняет письма от неизвестных отправителей.

Законные почтовые серверы повторяют попытку отправки позже, а спамеры — обычно нет.

Уменьшает количество спама без сложной настройки.

SpamAssassin

Открытое ПО для фильтрации спама.

Использует байесовские алгоритмы, SPF, DKIM, DNSBL.

Работает на уровне почтового сервера и поддерживает гибкую настройку правил.

Проверка DNS-записей и PTR-записей (reverse DNS).

Настройки Postfix:

Список источников

reject_unknown_client_hostname

reject_non_fqdn_helo_hostname

reject_unknown_sender_domain

reject_unverified_sender

Логирование и тестирование через telnet или swaks.

Выводы

Фильтрация спама должна быть многоуровневой.

Комбинация SPF, Greylisting и SpamAssassin значительно повышает эффективность защиты.

Правильная конфигурация SMTP сервера снижает риски фишинга и заражений.

Список источников

Klensin J. Simple Mail Transfer Protocol. RFC 5321.

The Next Step in the Spam Control War: Greylisting — Evan Harris, 2003.

Документация SpamAssassin — https://spamassassin.apache.org/

Статьи о фильтрации на Habr и Mail.ru Tech.